ADAPTING EMERGENGY MANAGEMENT SOFTWARE TOOLS TO CRITICAL INFRASTRUCTURE PROTECTION NEEDS

Risk and Threat Assessment Technologies Session
15th Annual NDIA Security Technology Symposium & Exhibition
Norfolk, Virginia
June 16, 1999

Prepared by:

Paul Byron Pattak
President
The Byron Group, Ltd.
Post Office Box 22817
Alexandria, Virginia 22304

703.751.6138 (o)
703.751.5154 (f)

pattak@tmn.com

ADAPTING EMERGENCY MANAGEMENT SOFTWARE TOOLS TO CRITICAL INFRASTRUCTURE PROTECTION NEEDS

1.0 ABSTRACT

Software tools developed for crisis and emergency management requirements can be easily adapted to meet the needs of *Critical Infrastructure Protection* (CIP)[1]. These emergency management software tools (EMSTs) can be used to create and maintain flexible knowledgebases to manage data for a variety of security and emergency scenarios.

- First, these EMSTs can be used as *mitigation* and *preparedness* tools for recording ongoing plans, procedures and identifying existing hazards and vulnerabilities.

- Second, the EMSTs can provide *mission-critical* operational data during actual crisis responses and post-event after-actions.

- Third, EMSTs can be used as *decision information* tools to develop sound risk management strategies and build business cases for acquiring the necessary resources to increase and ensure critical infrastructure protection.

Many discussions of crisis and emergency management technology tools focus only on their usefulness for event-specific actions, i.e. that they are only useful for planning and responding to an emergency. This paper endorse the notion of taking EMSTs further and using them in an ongoing critical infrastructure protection *operational* context, a post-event *reconstitution* context, and an *after-action* context for lessons learned. Finally, the paper shows how these EMSTs can be used to make better decisions for the planning, funding and use of various security-related resources.

These technologies are available today, and can be quickly put to work by those who are charged with protecting people, physical assets and information. Thus, enterprises can realize significant savings in time and resources by leveraging existing technology in a dual-use fashion to meet their security and critical infrastructure protection responsibilities[2].

---

[1] The President's Commission on Critical Infrastructure Protection (PCCIP) was created by Executive Order 13010 of July 15, 1996. The PCCIP submitted its Final Report in October 1997. The Report significantly raised awareness within government and private industry on a new set of issues which may affect people, companies and their respective resources. For a copy of the Report and other information as well as the latest information on the Federal Government's initiatives, please reference the following two websites: *www.pccip.gov* and *www.ciao.gov*.

[2] For Federal agencies, these are defined by Presidential Decision Directives 62 and 63 of May 22, 1998. For private industry, the equivalent responsibilities are in accordance with sound corporate risk management principles.

For purposes of this paper, the term "critical infrastructure protection" will be used to include, but not be limited to, those policies, procedures, tools and programs which:

- *Provide physical protection* to people and physical assets of an enterprise;
- *Protect critical data* and the information systems which store the data;
- *Maintain reliability* of critical enterprise systems; and
- *Enable reconstitution* of an enterprise if operations are disrupted.

2.0 HISTORY AND DEVELOPMENT OF EXISTING SOFTWARE TOOLS

Existing software tools for crisis and emergency management have been developed over approximately the last quarter century and currently represent a high level of sophistication. The development of these tools began in earnest when the popular notion of disasters – particularly weather-related disasters began to change. Some information had been compiled and managed in an organized fashion during the 1950's and 1960's– but most of it was in support of national, state and local civil defense programs and activities. Natural disasters were seen for the most part as "acts of God" which could only be endured to one extent or another, and which could be planned for, but not with universally-accepted principles and therefore, universally-useful information systems.

Several things happened in during the 1970's to change this notion. One significant event was Hurricane Agnes in 1971 during which the Federal Government responded differently than it had before. Typical Federal responses previous to Agnes had been sporadic and localized. After Agnes hit, the President appointed the first Federal Coordinating Officer (FCO) to coordinate resources across all Federal agencies in responding to a disaster[3].

Another significant event was a study by the National Governor's Association (NGA) in 1977, which concluded that all emergencies (natural, man-made, technological) have certain common discrete stages, and thus could be planned for and managed. This changed the way emergencies were viewed and led to a more systematic approach in the form of "emergency management." This was further developed into the notion of Comprehensive Emergency Management (CEM) and the recognized four phases of an emergency[4]:

- *Mitigation* (reducing or eliminating either probability or effects of an emergency)
- *Preparedness* (development of plans, training exercises, etc.)

---

[3] In an interesting historical footnote, this first FCO was Frank Carlucci who later went on to serve with distinction in several Administrations over the next two decades and concluded his government career as Secretary of Defense in President Reagan's second term.

[4] During its term, the President's Commission on Critical Infrastructure Protection (PCCIP), determined that there were five infrastructure assurance functions (policy formulation, prevention and mitigation, information sharing, incident management and consequence management). These five functions are relevant when looking at all the entities which constitute the partnership needed to respond to specific events whose effects go beyond the original enterprise.

- *Response* (provision of direct services, victim assistance, limiting additional damage)
- *Recovery* (clean-up, returning to normal, economic re-development)

The four phases constituted an on-going cycle which theoretically would lead to increasingly improved emergency management capability because of the lessons learned with each event. The NGA study defined CEM very clearly: "…Comprehensive Emergency Management (CEM) is a new term. It refers to a state's responsibility and capability for managing all types of emergencies and disasters by coordinating the actions of numerous agencies. The "comprehensive" aspect of CEM includes all four phases of a disaster or emergency activity: mitigation, preparedness, response and recovery. It applies to all risks: attack, man-made, and natural, in a federal-state-local partnership…A CEM program identifies agencies and individuals who have useful resources to bring to bear upon all aspects of emergencies."

Finally, the President established[5] the Federal Emergency Management Agency (FEMA) on April 1, 1979 by combining several independent agencies and offices which had been scattered throughout the Federal Government. One original intent of FEMA was to provide "one-stop shopping" for coordination and provision of emergency management services at the national level.

The combined result of these events drove the requirement for automated information management tools, and the necessary software to make them a reality. Various emergency management software publishers then developed commercial off-the-shelf (COTS) products which worked on microcomputers, were designed around emergency management processes and were intuitive and easy to use.

2.1 Mitigation and Preparedness Tools

The first necessary use of EMSTs is to develop them as mitigation and preparedness tools for an enterprise. This means entering basic planning data for the full range of emergency contingencies. This data includes:

- Personnel rosters, name, rank and serial number;
- Training and certification (HAZMAT, CPR, etc.) information;
- Detailed floor plans;
- Maps, wiring diagrams, plumbing diagrams, HVAC diagrams, etc.;
- Inventories;

[5] The President signed Reorganization Plan Number 3 of 1978 to accomplish this. FEMA does not have a legislative charter – i.e. it was not created by an Act of Congress.

- Material Safety Data Sheets (MSDS);
- Emergency operations plans, procedures, (SOPs), checklists; other documents;
- Call-down systems;
- Plume models, dispersal models, etc.;
- Legal and regulatory information; and
- Census information.

This information can be stored in word processing documents, spreadsheets, databases, project management templates or graphics documents.

The data are then updated as needed, and used in exercises and simulations to test the enterprise's ability to respond to an emergency event.

APPLICABILITY TO CRITICAL INFRASTRUCTURE PROTECTION: A central tenet of CIP is for an enterprise to understand where it is potentially vulnerable and what resources are available in response. An enterprise also needs to understand what its inter-dependencies are to other enterprises – and EMST is a good place to record this information. Also, EMSTs can store valuable data beyond that which can be directly used for emergencies – enterprises should broaden the amount of information for CIP which is kept in such a system.

2.2 Mission-Critical Operational Data

The second category of information is that which is mission-critical and can actually be used during a response to an emergency event. EMSTs often contain guidelines for how to apply procedures, personnel and resources during an event. A key element is for procedures, personnel and resources to be applied quickly during an event – having the information listed in the previous section in one place makes this possible. In addition, the following can be accomplished:

- *Procedures, Personnel and Resources* These can be marshaled and directed with greater efficiency during an event, and targeting them as appropriate.
- *Communications Capability* EMSTs can contain communications modules which permit the transmission and sharing of critical data between the enterprise, public safety agencies and others. Capability includes telephone, fax, packet radio, re-broadcasting of weather data, video, e-mail and the Internet.
- *Mapping Capability and Models* The maps combined with modeling capability can facilitate the direction of response resources to those areas which may have to deal

with a release of toxic material into the atmosphere. Another good example is the ability to make evacuation decisions. Mapping capability and models can also be used to literally "direct the traffic" for response resources otherwise.

APPLICABILITY TO CRITICAL INFRASTRUCTURE PROTECTION: These capabilities can be used for day-to-day operations and to ensure ongoing reliability, rather than just being invoked during an emergency situation. The use of EMSTs can be broadened into more areas which complement emergency preparedness and management – the capability already exists.

2.3 Decision Information Tools

When used to their fullest capacity, EMSTs are used by enterprises as decision information tools both before and after emergency events. When they are used before an event, the compilation of all the information in the various types of databases allows management to see potential shortfalls in emergency response resources and procedures – and to quantify what needs to be done to correct the situation. When used afterwards, EMSTs can be valuable tools by examining what went right and what went wrong during the event – particularly with an eye toward improving what may have gone wrong. This latter item is because the data contained in an EMST can help quantify potential shortfalls.

APPLICABILITY TO CRITICAL INFRASTRUCTURE PROTECTION: Constant analysis of procedures and resources is integral to CIP. The ever-expanding databases within the EMST become more valuable over time as they come to include historical data. The combination of planning and operational data with historical data will allow management to test assumptions, exercise plans, make reasonable predictions of performance and analyze capability. The data also exists upon which to build the business cases to secure the necessary resources for CIP (and emergency management). All of this, when done in an organized fashion, can lead to improved decision-making.

3.0 STRATEGIES AND RECOMMENDATIONS

Many discussions of crisis and emergency management software tools focus only on planning and response activities. This is not in and of itself a bad thing – particularly since planning and response are such critical element of crisis and emergency management. However, the potential uses of EMSTs go far beyond planning and response and can involve significant other areas of what is termed "critical infrastructure protection" and infrastructure assurance[6]. This section addresses some of those areas.

[6] Infrastructure assurance (IA) is a broader term beyond critical infrastructure protection (CIP) even though the two are often used interchangeably. CIP focuses more on the actual physical and electronic protection of people and resources. IA goes beyond that to incorporate more formal risk management, the ability to restore the provision of products and services, and the ability to reconstitute after a negative event. Definitions for CIP and IA are highly subjective (these particular definitions reflect the author's perspective), and there is no uniformity at this time among government and private industry.

3.1 Operational

In the context of critical infrastructure protection, "operational" means the day-to-day activities which provide products or services for the enterprise's customers. It will be very important for those with CIP responsibilities to thoroughly understand what their enterprises do – and be conversant in those activities. In order to prepare the enterprise against various contingencies, they need to know about the business processes and process flows of the organization. To be beneficial to the operations managers, they need to demonstrate the value of integrating everyday, common sense security and emergency management precautions into the daily operational activities of the enterprise. One example might be the recording of enterprise-wide incident and maintenance logs in the EMST. From this and other actions, security and emergency management activities are seen as "mainstream" rather than just another burden which needs compliance activity and resources.

Thinking in operational terms leads to more relevant vulnerability assessments. A mere cataloguing of the entire universe of possible threats would overwhelm any system. It is vital that the assessment record those vulnerabilities and inter-dependencies which affect either operations or the ability to resume operations. This focus makes it easier to quantify potential problems – and solutions.

EMSTs make it possible to record the business processes and the potential vulnerabilities and store the relevant data within the same system as the contingency plans themselves. The real value of this approach to make contingency planning an enterprise project which involves more people than the current security or emergency management paradigms. The constant accumulation of data from multiple sources and the way in which it is combined turns mere databases into knowledgebases. All of this leads to more robust critical infrastructure protection.

3.2 Reconstitution

There are many useful things EMSTs can be used for in a post-event scenario. The most relevant are those which facilitate resumption of normal activities by all concerned. A brief listing includes, but is not limited to:

- Facilitating damage assessment to quantify extent of loss;
- Use of Geographic Information Systems (GIS) to permit visualization of damage;
- Providing the data for a variety of briefings;
- Checklists for post-event actions and restoration of service;
- Providing updated information to customers and stakeholders;
- Provision of databases, e.g. resources needed to reconstitute or backup data tapes;
- Tracking alternative suppliers, sources, Plan "B" activities, etc.; and
- Organizing information relating to back-up hotsites and alternate command centers.

EMSTs can be just as valuable after an event as they were before and during – it is all a matter in how they are used. Their post-event value comes from increasing how quickly an enterprise can resume providing products and services to its customers. In private industry, this can literally mean the difference between life and death for an enterprise. Again, if configured as knowledgebases with the relevant data at hand, EMSTs permit the enterprise's leadership to make quicker and better decisions about restoration of services.

3.3 After Action

As the reconstitution is well underway, the enterprise needs to determine what courses of corrective action it needs to take to minimize the potential for such damage in the future. More importantly, the after action activities should be part of a larger effort of continuous improvement and the ongoing incorporation of best practices by an enterprise. In this respect, EMSTs are useful in the following areas:

- Review of event message traffic to search for possible improvements;
- Input to re-creating the event and responses;
- Using this input in exercises and simulations;
- Designing "what-if?" scenarios based on actual events;
- Experimentation with alternative response paradigms;
- Development of inter-operability with other enterprises, public safety agencies; and
- Frequent testing of systems for reliability.

Most of what is in the above list is familiar to emergency management and security professionals. On the other hand, operations managers and the enterprise's leadership need to know the value of such activities and the case for being prepared needs to me made before an event. All the after action activities need to be thought out in advance and be ready for implementation as soon as possible after the event. However, what differentiates CIP thinking from traditional thinking is that "after action" events should be going on continuously.

3.4 Making the Business Case for CIP Resources

The people, tools and resources necessary to effect a good CIP program for an enterprise will not exist if management does not provide the necessary funding. To do so requires design, development and preparation of the necessary business cases. For too often, emergency management and security professionals have operated under the assumption that because "they were doing good, they should be doing well." Another way of looking at it was that they should be funded and supported simply because they were doing the right thing. In today's world however, funding and resources often go to those who can articulate the best need and justification. The need and justification in turn, often have to be quantified – and that is where the EMST can come handy for the following reasons:

- Most of the necessary data for the business case are in the EMST;

- What the funding purchases can easily be quantified;
- Relevant management information requirements should already be in the system;
- Detailed analysis of past actions can be produced;
- Reasonable predictions and scenarios can be developed;
- Proposed iterative improvements can be shown and tracked; and
- CIP resource needs can be *quantified*.

Building a business case is particularly relevant in the for-profit world, but can be equally valid in a resource-constrained not-for-profit environment. What EMSTs (configured as knowledgebases) permit the emergency management and security professional to do is to more easily collect the necessary data and develop the resulting arguments in support of the funding needed to provide an adequate level of CIP funding. Correspondingly, by showing CIP activities as being integral to enterprise operational activities, it can change the mindset of management from looking at emergency management and security as "necessary evils" to looking at them as an indispensable part of operations capability.

4.0 CONCLUSIONS

There are three key points for the adaptability of EMSTs to critical infrastructure protection.

4.1 EMSTs Are Ideal for Critical Infrastructure Protection

EMSTs evolved into useful data collection and management mechanisms for tracking, maintaining and providing critical information before and during an emergency event. For the purposes of critical infrastructure protection, their use can be expanded into even more sophisticated knowledgebases which track and maintain a much broader range of data – and which are used much more frequently in an operational environment. Used for a full range of critical infrastructure protection functions, EMSTs can become an even more integral part of enterprise operations.

4.2 Existing EMSTs Are Adaptable for Critical Infrastructure Protection

The software tools necessary to address security and critical infrastructure protection needs already exist in usable form. Adapting them to specific applications and circumstances requires only will and creativity. And by adapting existing tools, tremendous savings in time and expense can be realized by enterprises who wish to protect their people, assets and resources.

4.3 Opportunity Exists for Emergency Management and Security Professionals

Adapting EMSTs for critical infrastructure protection and infrastructure assurance represents a new opportunity for emergency management and security professionals. First, they have the chance to make their existing software tools more relevant for a new

and expanding domain of public policy. Second, they have the opportunity to work more closely with their colleagues in enterprise operations – a collaboration which will benefit both. Finally, these professionals have the opportunity to bring emergency management and security issues to the boardroom in ways which have not been possible before.

For more information:

Mr. Pattak is an educator, speaker and consultant in policy and technology matters for corporate and government clients. He practices the art of personal and institutional diplomacy between the technical and non-technical worlds, and assists clients in adopting technological advances without sacrificing the quality of the working environment for their employees. His current focus areas are in the development of critical infrastructure assurance technologies, policies and strategies; helping organizations adapt to new technology trends, facilitating the transfer of dual-use technologies into domestic civilian applications; and the use of technology to improve emergency management and disaster planning activities by government and the private sector.

Mr. Pattak's clients have included the President's Commission on Critical Infrastructure Protection (where he served as a Senior Consultant), the Critical Infrastructure Assurance Office, the National Academy of Sciences, the National Security Council, the Executive Office of the President, the Department of the Treasury, the Department of Defense, the Department of Interior, the Department of Agriculture, the Department of Transportation, the Department of Energy, the Federal Emergency Management Agency, the Defense Threat Reduction Agency, the International Monetary Fund, IBM, TRW, B. F. Goodrich, Goodyear, Marathon Oil,Bank One, The Limited, KeyCorp, LTV Steel, Owens Corning, VanStar and PEPCO. In addition, Mr. Pattak has been a lecturer at the National Defense University and at the U.S. Army War College on infrastructure assurance. He has also spoken on many topics to various government and private audiences in the Washington, DC metro area.

Mr. Pattak has also served in the Federal Government as a political appointee at the Federal Emergency Management Agency during President Bush's Administration; as a Management Intern within the Office of the Secretary of Defense; and as an Office Assistant at the National Institutes of Health.

Paul Byron Pattak
President
The Byron Group, Ltd.
Post Office Box 22817
Alexandria, VA 22304

703.751.6138 (office)
703.751.5154 (fax)

pattak@tmn.com (e-mail)

